UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/814,319	03/21/2001	Jorg Gregor Schleicher	2030P	3776

7590   09/09/2004

SAWYER LAW GROUP LLP
P. O. Box 51418
Palo Alto, CA   94303

EXAMINER
DADA, BEEMNET W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _21 March 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-32_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-32_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _2_.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-32 have been examined.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al.

(hereinafter referred to as Scott) (US Pub. No. 2002/0049760 A1) in view of Farber et al.

(hereinafter referred to as Farber) (US Patent No. 5,978,791).

4.   As per claim 1 and 16, Scott teaches, a method for electronically delivering files over a

public network of computers comprising at least one server node and multiple client nodes, the

method comprising the steps of:

enabling secure and reliable peer-to-peer file sharing between two client nodes (page 1,

paragraph 0007) by,

generating and associating a digital fingerprint (i.e., hash id) with a file in response to the

file being selected for publication on a first client node [page 2, paragraph 0026, and page 3,

paragraph 0032];

adding an entry for the file to a searchable index of shared files on the server node and storing the fingerprint on the server [page 4, paragraph 0042 and 0044];

in response to a second client selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node [column 4, paragraph 0047]. Furthermore, Scott teaches generating a fingerprint (hash code) of the file for uniquely identifying the file using different implementation methods such as MD5 and SHAI [page 3, paragraphs 0032 and 0033]. Scott does not explicitly teach generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher. However, generating and comparing a fingerprint of a file with a previously generated fingerprint to determine the authenticity of the file and publisher is well known in the art. For example, in the same field of endeavor Farber teaches a peer-to-peer file sharing network including generating fingerprint of a file for authentication [column 12, lines 54-67 and column 13, lines 1-18]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a method of generating a new fingerprint for a file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher as per teachings of Farber and incorporate it into the peer-to-peer file sharing system of Scott, because the method further enhances the system by verifying the authenticity of the file and publisher using fingerprint of the file.

5.   As per claims 31 and 32 Scott teaches a method for electronically delivering files over a public network of computers comprising at least one server node and multiple client nodes, the method comprising the steps of:

enabling secure and reliable peer-to-peer file sharing between two client nodes (page 1,

paragraph 0007) by,

generating and associating a digital fingerprint (i.e., hash id) with a file in response to the

file being selected for publication on a first client node [page 2, paragraph 0026, and page 3,

paragraph 0032];

adding an entry for the file to a searchable index of shared files on the server node and

storing the fingerprint on the server [page 4, paragraph 0042 and 0044];

in response to a second client selecting the file from the search list on the server node,

automatically transferring the file from the first client node directly to the second client node

[column 4, paragraph 0047].

enabling subscription-based decentralized file downloads to the client nodes by allowing

the client nodes to subscribe with the server node to periodically receive copies of one of the

files, when providing a current subscribing client node with the file, locating the closest client

node containing the file, and transferring the file from the closest node directly to the current

subscribing node, thereby efficiently utilizing bandwidth [page 4, paragraph 0046-0049 and

page 3, paragraph 0034]. Furthermore, Scott teaches generating a fingerprint (hash code) of the

file for uniquely identifying the file using different implementation methods such as MD5 and

SHAI [page 3, paragraphs 0032 and 0033]. Scott does not explicitly teach generating a new

fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node

to determine the authenticity of the file and publisher. However, generating and comparing a

fingerprint of a file with a previously generated fingerprint to determine the authenticity of the file

and publisher is well known in the art. For example, in the same field of endeavor Farber

teaches a peer-to-peer file sharing network including generating fingerprint of a file for

authentication [column 12, lines 54-67 and column 13, lines 1-18]. Therefore it would have been

obvious to one having ordinary skill in the art at the time the invention was made to include a method of generating a new fingerprint for a file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher as per teachings of Farber and incorporate it into the peer-to-peer file sharing system of Scott, because the method further enhances the system by verifying the authenticity of the file and publisher using fingerprint of the file.

6.   As per claims 2 and 17, the combination of Scott and Farber teaches the method as applied above. Furthermore, Scott teaches, enabling subscription-based decentralized file downloads to the client nodes by allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files, when providing a current subscribing client node with the file, locating the closest client node containing the file, and transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth [page 4, paragraph 0046-0048 and page 3, paragraph 0034].

7.   As per claims 3 and 18, the combination of Scott and Farber teaches the method as applied above Furthermore, Scott teaches generating a fingerprint (hash code) of the file for uniquely identifying the file using different implementation methods such as MD5 and SHAI [page 3, paragraphs 0032 and 0033]. The combination of Scott and Farber fails to teach generating digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key. However Official notice is taken that it is old and well known in the art to generate a digital certificate that includes a private key and public key. It would have been obvious to have included a method of generating a digital certificate within the

combination of Scott and Farber as digital certificates are known to provide secure public/private key encryption and verification methods.

8.   As per claims 4-6 and 19-21, the combination of Scott and Farber teaches the method as applied above. Furthermore, Scott teaches generating a fingerprint (hash code) of the file for uniquely identifying the file using different implementation methods such as MD5 and SHAl [page 3, paragraphs 0032 and 0033].

9.   As per claims 7 and 22, the combination of Scott and Farber teaches the method as applied above. Furthermore, Scott teaches the method further including the step of providing the server node with a database for storing the user's account information and the fingerprint for the file [page 4, paragraph 0042 and 0044].

10.   As per claims 8 and 23, the combination of Scott and Farber teaches the method as applied above. Furthermore, Scott teaches the method further including the step of transferring the file from the first client node directly to the second client node if both the first and second client nodes are logged-in to the network and no firewall separates the first and second client nodes [column 4, paragraph 0047].

11.   As per claims 9 and 24, the combination of Scott and Farber teaches the method as applied above. Furthermore, Scott teaches the method further including the step of if the second client node is not logged into the network, then temporarily storing the file on the server node, and delivering the file by the server node when second client node logs-in to the network [column 4, paragraphs 0046 and 0047].

12.   As per claims 10 and 25, the combination of Scott and Farber teaches the method as

applied above. Furthermore, Scott teaches the method further including the step of: if a firewall

separates the first client node from the second client node, then using the server node to act as

a proxy for the second client node and sending the file through the server node [page 4,

paragraphs 0046-0049].

13.   As per claims 11 and 26, the combination of Scott and Farber teaches the method as

applied above. Furthermore, Scott teaches the method further including for allowing a user of

the first client node to search for files on the network, and presorting results based on files found

that are stored on client nodes located closest to the first client node [page 4, paragraph 0044].

14.   As per claims 12 and 27, the combination of Scott and Farber teaches the method as

applied above. Furthermore, Scott teaches the method further including the step of transferring

the file during off-peak hours to take advantage of idle bandwidth of the subscribing node and

thereby evening out bandwidth distribution of the network [pages 4 and 5, paragraph 0049,

0050].

15.   As per claims 13 and 28, the combination of Scott and Farber teaches the method as

applied above. Furthermore, Scott teaches the method further including the step of allowing a

user of the first client node to privately publish the file or publicly publish the file [page 3,

paragraph 0032].

16.   As per claims 14 and 29, the combination of Scott and Farber teaches the method as

applied above. Furthermore, Scott teaches the method further including transferring a copy of

the file from the first node to the server node so that should the first node be off-line when

another node request the file, the file may then be served by the server node [pages 4 and 5,

paragraph 0049].

17.   As per claims 15 and 30, the combination of Scott and Farber teaches the method as

applied above. Furthermore, Scott teaches the method further wherein step of transferring the

file to the second client node further includes the step of transferring different portions of the file

from different nodes and then reassembling the file upon receipt [pages 4 and 5, paragraphs

0049,0050].

Conclusion

18.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure. See PTO Form 892.

        Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The

examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).
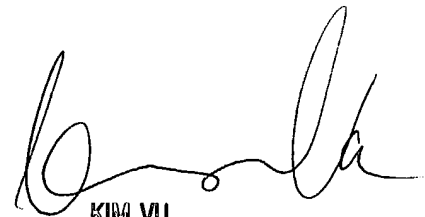
        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

September 2, 2004

KIM VU
SUPERVISORY PATENT EXA:
TECHNOLOGY CENTER 2: